EXHIBIT A

LIU.6261

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

QUINN LUNDGREN EAKER	§	
	§	
	§	
V.	§	
	§	**CIVIL ACTION NO.**
	§	**4:14-cv-00443-O-BJ**
SECURE COLLATERAL	§	
MANAGEMENT,	§	
MARY MOORE,	§	
MARK NEWMAN	§	

AFFIDAVIT OF JIM FARLEY

STATE OF	§
	§
COUNTY OF	§

BEFORE ME, the undersigned authority, personally appeared Jim Farley who, being by me duly sworn, deposed as follows:

1. "My name is Jim Farley. I am over eighteen (18) years of age and I am a resident of the state of Texas. I am the Principal and C.F.O. of Secure Collateral Management, LLC ("Secure Collateral"). I am fully competent to make this Affidavit. I have personal knowledge of the facts stated herein and they are all true and correct."

2. As Principal and C.F.O. of Secure Collateral I have personal knowledge of the relationship between Secure Collateral and Plaintiff Quinn Eaker. Further, I have personal knowledge of the business operations of Secure Collateral, including services Secure Collateral provided related to collateral possessed by Quinn Eaker.

3. With regard to Quinn Eaker, Secure Collateral contracted with T.D. Auto Finance, LLC to provide skip-tracing services related to a 2012 Toyota Prius VIN #JTDKN3DPXC3011576 (the "Collateral"). A true and accurate copy of the Collateral Locate Agreement by which Secure Collateral was retained to provide skip-tracing services is attached hereto as Exhibit "A-1". Secure Collateral received the assignment pertaining to Quinn Eaker on or about April 29, 2014.

4. Pursuant to the Collateral Locate Agreement, Secure Collateral would receive payment following a successful locate of subject collateral. *See* Exhibit A-1. Secure Collateral would also receive payment if the subject collateral was ultimately repossessed. *See* Exhibit A-1. This payment arrangement is usual and customary in the business of skip-tracing.

5. Skip tracing services involve the location of collateral via information obtained by

computerized searches. Secure Collateral then verifies the information received from computerized searches by making phone contact with persons identified via the aforementioned searches.

6. Secure Collateral does not solicit or arrange for payments of outstanding debts. Rather, if a debtor brings up payment related to a debt, the debtor is referred to the bank or noteholder.

7. At no time was Secure Collateral retained to provide repossession or debt collection services related to Quinn Eaker. Rather, Secure Collateral engaged only in information gathering and message delivery.

8. No employee of Secure Collateral visited the property occupied by Quinn Eaker, nor did any employee of Secure Collateral attempt to gain control of the Collateral.

9. Secure Collateral was not able to make contact with Quinn Eaker. Though attempts to reach Plaintiff in order to obtain his contact information were made, Secure Collateral was limited to leaving a voicemails for Mr. Eaker on May 19, 2014 and May 30, 2014. Mr. Eaker did not personally return said messages.

Further Affiant sayeth not.

SIGNED this ___ day of March, 2015.

J Farley
____
JIM FARLEY

SUBSCRIBED AND SWORN TO BEFORE ME on this 27 day of March 2015 to certify which witness my hand and seal of office.

Homer H Miller
____
Notary Public in and for
The State of Texas

My Commission Expires:
3-17-2017

HOMER H. MILLER
NOTARY PUBLIC, STATE OF TEXAS
MY COMMISSION EXPIRES
MARCH 17, 2017

NOTARY PUBLIC STATE OF TEXAS

EXHIBIT A-1

Collateral Locate Services Agreement

This Collateral Locate Services Agreement ("Agreement") is entered into as of October 1, 2012 ("Effective Date") between TD Auto Finance LLC ("TDAF"), located at 27777 Inkster Road, Farmington Hills, MI 48334-3125, and Secure Collateral Management, LLC ("Provider"), located at 12620 E. Northwest Hwy Dallas Tx 75228

A. TDAF is considering placing with Provider TDAF accounts arising from certain retail installment contracts, lease agreements, promissory notes and security agreements or other finance, lease or loan agreements, that have an outstanding balance due to TDAF ("Account" or "Accounts"); and

B. Provider is willing to accept such placements and to locate the outstanding collateral on a contingency basis for the benefit of TDAF under the terms of this Agreement.

Therefore, the Parties agree as follows:

1.0 **Assignment of Accounts.**

1.1 Accounts are placed with Provider for the sole and limited purpose of locating TDAF's customers, vehicles leased or purchased under contract with TDAF, or persons in possession of vehicles leased or purchased under contracts with TDAF.

1.2 All Accounts placed by TDAF with Provider are and shall continue to be the exclusive property of TDAF and are placed with Provider only for the purpose of collateral location. Provider shall not acquire any right or interest in the Accounts and notwithstanding any provision of federal, state or local statutory or common law Provider shall not acquire nor assert any claim or interest, including possessory or non-possessory lien rights, in the Accounts, the related collateral, related files or other documents submitted to Provider or otherwise received by Provider in connection with the referral of any Account or in the proceeds of any Account.

1.3 Any Account assigned to Provider will not be assigned to another Provider while Provider is in possession of the TDAF Account.

1.4 Referral of Accounts shall be at the sole discretion of TDAF.

2.0 **Services.** Provider agrees to perform the services outlined in Exhibit A (the "Services")

3.0 **Term and Payment for Services.**

3.1 TDAF will pay Provider a contingency fee if one of the following events occurs within the timeframe set forth in Exhibit B:

(a) Successful repossession or confirmed location of collateral securing the Account.

(b) Subject to the terms in Section 4 of this Agreement, and while the Account is assigned to Provider, payment in full or settlement in full is received by TDAF due to the Provider's efforts

3.2 Provider agrees that no fee or costs other than the contingency fee in Exhibit B shall be billed to TDAF unless otherwise agreed to in writing by an authorized TDAF Skip Recovery Representative.

4.0 Provider Obligations.

4.1 Provider agrees to use only lawful and proper means to locate TDAF's customers and vehicles. Without limiting the foregoing, Provider specifically agrees that at no time will Provider, its employees, representatives or agents:

(a) Engage in activities constituting "pre-texting" of any nature whatsoever. Pre-texting includes any use of false, fictitious or fraudulent statements or documents to obtain information about a customer, using forged, counterfeit, lost or stolen documents to obtain customer information from the customer or from third parties, or requesting another person to obtain customer's information using false, fictitious or fraudulent statements or document;

(b) Make false or deceptive statements, whether written or oral, or misrepresent in any manner whatsoever the identity or company affiliation of such person while performing any Services with respect to the Accounts;

(c) Otherwise use false pretenses or impersonation to obtain otherwise confidential information in the performance of Services on referred Accounts; or

(d) Engage in negligent use or unauthorized access of any system or software provided by TDAF or its authorized third party provider.

4.2 Provider agrees that it and any third party that it may retain under the terms of this Agreement will comply fully and strictly with all applicable federal, state and local laws and regulations in locating the vehicles, the TDAF customer(s) and in effecting repossession. TDAF forbids the use of any measures or tactics that violate any laws, including personal harassment or unconscionable threats. Under no circumstance may Provider threaten legal action, including civil or criminal prosecution of claims, in connection with the performance of the Services

4.3 Provider will exclusively use repossession companies or repossession forwarding companies approved by TDAF

4.4 Provider shall not report Account activity to any credit-reporting agency.

4.5 Provider is not authorized to commence litigation in regard to any Account.

4.6 Provider is prohibited from requesting payment from TDAF's customers or any other party in possession of a vehicle subject to an Account.

4.7 If any customers or parties in possession of vehicles subject to an Account offers payment without request or demand made by Provider, those customers or other parties shall be immediately referred to a TDAF Skip Recovery Representative.

4.8 All payments that are made voluntarily and without any explicit or implicit requests or demands made by Provider must be immediately forwarded to TDAF via next-day mailing at the following address:

TD Auto Finance
4600 Touchton Road
Building 200 Suite 400
Jacksonville, FL 32246
Att: Skip Recovery Group

Payment received by Provider on behalf of TDAF shall not be deposited in any Provider operating or escrow account.

5.0 **Termination.**

5.1 TDAF reserves the right to request the closing of, cessation of activity on, and return of any Account at any time after placement. Provider shall have 24 hours to remove the Account from their active system. There shall be no charge to TDAF for any such closed or recalled Account

5.2 Provider agrees to cease location activity and return placed Accounts no later than the first day after the placement period as set forth in Exhibit B. Recoveries of collateral generated subsequent to the placement period set forth in Exhibit B are not eligible for fee earnings with the exception of Accounts that have been approved by an authorized TDAF Skip Recovery Representative for retention beyond the placement period set forth in Exhibit B.

5.3 This Agreement may be terminated without penalty by either Party for any or no reason upon 30 days written notice prior to the desired termination date.

6.0 **TDAF Obligation.** TDAF will notify Provider of all payments made directly to TDAF on any Account that is placed with Provider at the time payment is made on Charged-Off Accounts.

7.0 **Insurance.**

7.1 **Insurance Requirements.** Provider warrants that it has insured against all losses, claims, demands, proceedings, damage, costs and expenses for injuries or damage to any person or property that are the result of the fault or negligence of Provider in the performance of this Agreement Provider agrees, at minimum, to maintain the following insurance coverage with insurance carriers:

(a) Workers' Compensation Statutory Limits for the state or states in which this order is to be performed (or evidence of authority to self-insure);

(b) Commercial General Liability (including Premises, Operations, Independent Contractors, Products/Completed Operations and Contractual Liability) $3,000,000 each occurrence;

(c) Automobile Liability (including owned, non-owned and hired vehicles) $3,000,000 each occurrence; and

(d) Professional/Errors and Omissions Liability insurance appropriate to the Supplier's profession. Coverage must be for a professional error, act or omission arising out of the scope of services shown in this order - $3,000,000 per occurrence.

All policies of insurance shall be written as primary policies, not contributing with or in excess of other coverage and shall name TDAF as an additional insured.

8.0 **Confidentiality.** Provider agrees to comply with the Confidentiality Standards listed in Exhibit C.

9.0 **Information Security Requirements.** Provider agrees to comply with the Vendor Security Policy listed in Exhibit D.

10.0 **Audit and Compliance Requirements.** Provider agrees to comply with the Audit and Compliance Requirements listed in Exhibit E

11.0 **General IT Requirements.** Provider agrees to comply with the General IT Requirements listed in Exhibit F.

12.0 Indemnification. Provider will indemnify TDAF and its affiliates and directors, officers, employees, agents and each of their respective successors and assigns, against all claims, liabilities, losses, damages, costs and expenses of any nature (including reasonable attorneys' fees and costs) arising out of the injury or death of any person or damage or loss of any property allegedly or actually resulting from or arising out of any negligent act or omission of Provider or its employees, agents, or subcontractors in connection with this Agreement.

13.0 Limitation of Liability. In no event shall either Party be liable to the other for any indirect, incidental, special, punitive, exemplary or consequential damages arising out of this Agreement, including lost profits, business interruption, loss of business information, or cover, even if such Party has been advised of the possibility of such damages This section does not apply to a Party's indemnification obligations or to any breach of confidentiality.

14.0 Business Continuity and Disaster Recovery.

14.1 Provider shall develop and maintain one or more contingency plans designed to minimize disruption of the Services Without limiting the foregoing, Provider shall maintain back-up procedures and systems, redundant systems and disaster recovery systems relating to the Provider's System.

14.2 Provider will supply TDAF with a copy of the plan, and will describe any additional business continuity, disaster recovery and testing requirements that are particular to the Services to be performed under this agreement and any Statement of Work

14.3 Provider will immediately notify TDAF upon the occurrence of any event that may cause a Business Interruption including any operational incidents that might impact Provider's performance of the Services in accordance with the Agreement, including the Service Levels.

15.0 Miscellaneous.

15.1 This Agreement may not be modified or amended except by a written instrument executed by both Parties.

15.2 Provider agrees to maintain complete and accurate records of all written and telephonic communication related to TDAF accounts

15.3 This Agreement does not create a joint venture, partnership or other formal business relationship or entity of any kind, or an obligation to form any such relationship or entity. Each Party is an independent contractor and not an agent of the other Party for any purpose, and neither has the authority to bind the other.

15.4 Should any provision of this Agreement be ruled invalid by applicable legal authority, such provisions shall be to that extent deemed omitted and the remaining terms of this Agreement shall remain in full force and effect.

15.5 This Agreement shall be governed by and construed in accordance with the laws of the State of Michigan without reference to choice of law doctrines.

15.6 This Agreement may be executed in counterparts and each counterpart, when so executed and delivered, shall be deemed to be an original and all such counterparts shall constitute one and the same instrument. This Agreement may be executed by facsimile or electronic signatures and such signatures will bind each Party as if they were original signatures.

15.7 This Agreement supersedes all prior agreements, promises, representations or inducements, whether written or oral, and embodies the Parties' complete and entire agreement with respect to the subject of this Agreement.

15.8 This Agreement in no way confers any rights or benefits of exclusivity on Provider, or limits or prohibits IDAF from performing itself, or using any Person other than Provider to provide, services that are substantially similar to, or that interface with, all or any part of the Services.

IN WITNESS WHEREOF, the Parties, by their duly authorized representatives, have executed this on the date noted above.

ID Auto Finance LLC

By:______________________________

Title:______________________________

[Vendor Name]
Secure Collateral Management llc

By: T Farley

Title: Principal C.F.O.

Exhibit A: Services

Pre Charge Off Assignments:

- Locate the collateral securing the assigned Account.
- Work with previously assigned repossession forwarding agency or advise if one needs to be assigned Any exceptions must be approved in advance by an authorized TDAF Skip Recovery Representative in the TDAF Jacksonville Customer Contact Center.
- All other services as outlined in the Skip Operations Guide provided to you at execution of this Agreement and updated at interim times during the term of this Agreement.

Post Charge Off Assignments:

- Locate the collateral securing the assigned Account.
- Work with previously assigned repossession forwarding agency or advise if one needs to be assigned. Any exceptions must be approved in advance by an authorized TDAF Skip Recovery Representative in the TDAF Jacksonville Customer Contact Center
- Provide within 12 hours of the repossession the condition and personal property reports of the repossessed vehicle, address from where the vehicle was repossessed, the TDAF customer's home address, telephone number(s), and, if known, their place of employment. Such notification shall be made in a manner directed by and at the discretion of TDAF.
- All other services as outlined in the Skip Operations Guide provided to you at execution of this Agreement and updated at interim times during the term of this Agreement.

Exhibit B: Fees and Placements

Contingency fees and Placement periods are as follows:

Pre Charge Off Assignments

Tier	Fee	Placement Period
N/A	Flat Fee $375	Up to account charge off or when the assignment is closed.

Post Charge Off Assignments

Tier	Fee	Placement Period
Primary	$450	90 days
Secondary	$600	90 days
Tertiary	$750	90 days
Quad	$900	120 days
Warehouse	Greater of $1000 or 10% of auction estimate	varies

Tier Definitions:

- Primary Tier Placement – Account never placed with Provider post charge off
- Secondary Tier Placement – Account placed one time prior for collateral location, post charge-off
- Tertiary Tier Placement – Account placed two times prior for collateral location, post charge-off
- Quad Tier Placement – Account placed three times prior for collateral location, post charge-off
- Warehouse Tier Placement – Accounts placed as an alternative to collection agency placement or sale

Other Payments:

- If an Account is resolved solely through TDAF's efforts, a lesser payment can be considered.
- In addition, resolution through TDAF initiated tools (i.e , License plate recognition) will be paid at a lower rate
- If the Provider confirms the location of the collateral assigned but TDAF chooses not to repossess, a flat fee of $190 will be paid.

Exhibit C: Confidentiality

1. **Confidential Information.** "Confidential Information" of a Party means all information of a Party or its licensors, suppliers or affiliates that is not generally known to the public that is disclosed by a Party (the "Disclosing Party") to the other Party (the "Receiving Party") or that is otherwise learned by or comes into the possession or knowledge of the Receiving Party in connection with the Services, including information that has been identified as being proprietary or confidential or that by the nature of the circumstances surrounding the disclosure or receipt, or by the nature of the information itself, would be treated as proprietary and confidential by a reasonable person. Confidential Information of a Party includes any financial information in any form or medium, and all information of or about an identifiable officer, director, employee, customer or potential customer, and any customer lists or customer data (collectively, the "Personal Information"). Personal Information includes all information regarding customers of TDAF, regarding third party consumers having contact with TDAF, and TDAF's employees, the confidentiality of which TDAF must maintain pursuant to applicable federal and state privacy laws, rules, and regulations, including Public Law 106-102, the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 and Federal Regulation P, and Massachusetts General Laws Chp. 93H and its implementing regulation, as amended.

2. **Use and Disclosure of Confidential Information by Receiving Party Representatives.**

(a) The Receiving Party will not use Confidential Information of the Disclosing Party for any purpose other than: (i) evaluating, implementing or, in the case of TDAF, receiving services or exercising contractual rights associated with the specific Services for which such information was disclosed; (ii) as otherwise approved in writing by the Disclosing Party; (iii) as otherwise permitted by this Agreement or any agreement that incorporates this Agreement by reference; or (iv) as otherwise permitted by law

(b) The Receiving Party will not disclose or provide access to any Confidential Information except as permitted by this Agreement.

(c) The Receiving Party will take appropriate steps to ensure Confidential Information is safeguarded: (i) in accordance with industry accepted best practices and standards used or observed by comparable companies; and (ii) by implementing and maintaining administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Personal Information designed to meet the objectives of § 501(b) of the Gramm-Leach-Bliley Act and its safeguarding standards

(d) The Receiving Party will restrict access to: (i) Confidential Information to those employees, affiliates, agents, advisors, consultants and other representatives of Receiving Party ("Representatives") who have a need to know for the purposes of the Services; and (ii) only the Confidential Information such Representatives need for such purpose and under obligations of confidentiality no less stringent than those contained in this Agreement. Representatives will use and disclose Confidential Information to third parties only to the extent the Receiving Party may use and disclose such information. The Receiving Party will be liable for any failure by its Representatives to comply with the terms of this Agreement.

(e) The Receiving Party will collect, use, store, disclose, dispose of, provide access to, and otherwise handle Personal Information received, collected or accessible to the Receiving Party in accordance with all privacy laws applicable to such information.

3. **Exceptions.** The provisions of Section 2 will not apply to any information that:

(a) the Receiving Party can establish, by documentary evidence, was already known by the Receiving Party at the time of initial disclosure by the Disclosing Party;

(b) becomes publicly known through no wrongful act of the Receiving Party or its Representatives, or any other person subject to a confidentiality agreement in favor of the Disclosing Party;

(c) is rightfully received from a third party without similar restriction provided that the third party did not come into possession of the Confidential Information as a result, directly or indirectly, of a breach of an obligation of confidentiality owed by any person to the Disclosing Party;

(d) the Receiving Party can establish, by documentary evidence, was independently developed by or on behalf of the Receiving Party without reference to the Disclosing Party's Confidential Information; or

(e) is approved for release by written authorization of the Disclosing Party.

The foregoing exceptions are not applicable to any Personal Information.

4. **Legal Obligation to Disclose.** Unless otherwise prohibited by law, if the Receiving Party becomes legally obligated to disclose Confidential Information, the Receiving Party will give the Disclosing Party prompt written notice sufficient to allow the Disclosing Party to seek a protective order or other appropriate remedy, and will reasonably cooperate with the Disclosing Party's efforts to obtain such protective order or other remedy at the Disclosing Party's expense, and in the event the Receiving Party is unable to do so, the Receiving Party will (so long as not prohibited by law from doing so) advise the Disclosing Party immediately subsequent to such disclosure. The Receiving Party will disclose only such information as is required, in the opinion of its counsel, and will use reasonable efforts to obtain confidential treatment for any Confidential Information that is so disclosed.

5. **Storage of Confidential Information.** Receiving Party will keep Disclosing Party's Confidential Information logically isolated from any data of its other customers or suppliers, so that: (a) Confidential Information is not commingled with third party data or disclosed in conjunction with any disclosure of third party data; and (b) Receiving Party can readily locate or return Confidential Information in accordance with this Agreement. Except where authorized by TDAF in writing, Provider will not collect, use, store, disclose, dispose of, provide access to or otherwise handle any TDAF Personal Information.

6. **Additional Obligations for Personal Information.** To the extent Provider will be given access to or be provided with any Personal Information for purposes of the Services:

(a) Provider will ensure that all Representatives engaged in the performance of the Services that may have access to Personal Information have been trained in privacy compliance;

(b) Provider will designate an employee who will be responsible for all Personal Information in Provider's possession or under its control and for ensuring that Provider complies with the provisions of this Agreement; and

(c) Upon request by TDAF, but not more than once in any calendar year during the term of the Services, Provider will deliver a statement signed by a senior officer of the Provider confirming to TDAF in writing that, in respect of the previous twelve month period: (i) Provider has developed and implemented privacy compliance processes designed to ensure Provider's compliance with this Agreement; and (ii) to the best of Provider's knowledge, after reasonable inquiry, Provider has complied with the requirements set forth in this Agreement, with the exception of those incidents of non-compliance communicated to TDAF in writing. TDAF or a third party authorized by it may, during normal business hours, from time to time on prior written notice, enter upon any premises of Provider at which Personal Information is stored or used and audit the procedures, processes and information pertaining to Provider's compliance with this Agreement.

7. **Unauthorized Disclosure of Confidential Information.** If there is any unauthorized access to, disclosure or loss of, or inability to account for, any Confidential Information of the Disclosing Party, the Receiving Party will promptly, and in the case of Personal Information immediately after becoming aware thereof: (a) notify the

Disclosing Party; (b) take such actions as may be necessary or reasonably requested by the Disclosing Party to minimize the disclosure or loss; and (c) cooperate with the Disclosing Party to minimize the effect of the disclosure.

8. **Ownership of Confidential Information**. All Confidential Information will remain the exclusive property of the Disclosing Party, and the Receiving Party has no rights, by license or otherwise, to use the Confidential Information except as expressly provided in this Agreement

9. **No Warranty**. Except as otherwise agreed in writing, no warranties of any kind are given by either Party with respect to the accuracy, appropriateness or completeness of information provided to the other

10. **Return or Destruction of Confidential Information**. Subject to the provisions of a Transaction document, upon the Disclosing Party's written request, the Receiving Party will promptly return or destroy, and verify in writing its destruction of, all material, in any form, embodying Confidential Information of the Disclosing Party. In carrying out any destruction, the Receiving Party will protect Confidential Information in accordance with the terms of this Agreement. Notwithstanding the foregoing, IDAF may retain: (a) any minutes of meetings, copies of notes, internal analyses, records and other materials that contain or reflect Confidential Information; (b) Confidential Information stored on its computer systems, e-mails, or other forms of electronic information retention; and (c) Confidential Information required for regulatory, legal and compliance purposes For greater certainty, the terms of this Agreement continue to apply to any such retained Confidential Information

11. **Injunctive Relief.** The Receiving Party acknowledges that disclosure or use of Confidential Information in violation of this Agreement could cause irreparable harm to the Disclosing Party for which monetary damages may be difficult to ascertain or be an inadequate remedy. The Receiving Party therefore agrees that the Disclosing Party will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Agreement.

12. **Entire Agreement; Amendment.** This Agreement constitutes the entire agreement between the Parties relating to the matters to which it pertains and may be amended or modified only with the mutual written consent of the Parties.

13. **Scope; Termination**. This Agreement is intended to apply to all Confidential Information that is disclosed by the Disclosing Party to the Receiving Party or that is otherwise learned by or comes into the possession or knowledge of the Receiving Party, whether prior to, on or subsequent to the date of this Agreement. Either Party may terminate this Agreement by providing written notice to the other. Notwithstanding the termination of this Agreement: (a) the obligations set out herein will continue to apply with respect to Confidential Information disclosed prior to receipt of such written notice for as long as the exceptions in Section 3 do not apply to such information.; and (b) this Agreement will continue to apply to any transaction document in accordance with the terms of the transaction document.

Exhibit D: Vendor Security Policy

The information security requirements outlined in this Vendor Security Policy (the "Schedule") are required of all Vendors, Service Providers or other third parties who perform data processing services or information technology services for TD Auto Finance or on whose system(s) TD Auto Finance proprietary or confidential information resides for any reason. The information security requirements in this Schedule are integrated into the underlying agreement to which they are attached (the "Agreement") between TD Auto Finance and the Vendor or Service Provider.

1. **Vendor Data Safeguarding**
   - The Vendor, Service Provider or third party (each, a "Vendor") shall implement adequate administrative, technical, and physical safeguards: (i) to ensure the security and confidentiality of TD Auto Finance information; (ii) to protect against any anticipated threats or hazards to the security or integrity of such information; and (iii) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to TD Auto Finance or to any of its customers. Vendor, at its own expense, shall develop, implement and maintain a proven system or methodology to audit for compliance with the requirements in the preceding sentence. TD Auto Finance may audit the Vendor's personnel and operations, and perform physical and electronic reviews, including a review of the Vendor's information technology infrastructure security, or review an independent audit provided by the Vendor, in order to monitor the Vendor's compliance with the information safeguarding requirements. The Vendor shall develop, implement, and maintain, at its own expense, appropriate mitigation strategies to address issues identified as a result of these reviews.

2. **Vendor Security Policy**
   - Vendor will have an information risk management policy that: (i) communicates management commitment and information security requirements to all levels of the organization; (ii) aligns with ISO 27002:2005; and (iii) has been approved and reviewed by management within the last 12 months.

3. **Vendor Third Party Security**
   - Vendor shall obtain TD Auto Finance approval of any third parties or subcontractors used by Vendor to perform its duties under the Agreement.
   - Vendor shall require such third parties and subcontractors by contract to comply with the obligations imposed on Vendor by the information security requirements in this Schedule.

4. **Vendor Human Resources Security**
   - Vendor will ensure that its administrators and users with access to TD Auto Finance information or systems used for TD Auto Finance are adequately trained in and required to comply with TD Auto Finance information security and data safeguarding requirements
   - Vendor will only provide its employees and subcontractors with the level of access required to fulfill the requirements of the Agreement.
   - Vendor will ensure that TD Auto Finance information is safeguarded by previsions in its Confidentiality or Non-Disclosure Agreements for internal employees and contractors for the protection of information.

5. **Vendor Physical and Environmental Security**
   - Vendor shall put physical protection controls in place to ensure that assets are physically secure
   - Vendor, upon completion of contractual requirements or termination of this Agreement, will return to TD Auto Finance all information, data, documents, storage media and duplications owned by TD Auto Finance which it received.
   - Vendor shall provide evidence and confirm in writing that all TD Auto Finance information has been returned and all information copies on storage media has been destroyed beyond recovery
   - Vendor will not duplicate or transfer data received from TD Auto Finance to other computers or storage media unless it is necessary in order to achieve the purpose of the Agreement.

6. **Vendor Communications and Operations Management**
   - Vendor shall perform continuous logging and monitoring of networks, systems, applications and security devices within its environment to identify patterns, practices or events that indicate the possible existence of unauthorized access, modification, or theft of TD Auto Finance consumer or corporate information.
   - Vendor shall ensure that all TD Auto Finance privacy-relevant HR and non-public personal information is stored encrypted on all mobile devices, as well as encrypted when in transit over computer networks or by physical package delivery.

7. **Vendor Access Control**
   - Vendor shall implement physical and logical access controls to restrict and limit access to TD Auto Finance information and systems used for TD Auto Finance to authorized users.
   - Vendor shall implement a process to ensure that access to systems, applications, and information is reviewed based on changes in employee responsibilities or termination.
   - Vendor will ensure that other clients and third parties cannot access TD Auto Finance information.
   - Vendor shall guarantee the outright and verifiable separation of TD Auto Finance information from other clients within its data processing systems and applications
   - Remote maintenance of hardware and software used by TD Auto Finance or of the information protected by this Agreement is only permitted if TD Auto Finance has consented to the remote maintenance and the systems used for remote maintenance are comprehensively protected against unauthorized and improper entry or access.

8. **Vendor Information Systems Acquisition, Development and Maintenance**
   - Vendor will ensure all systems development and infrastructure changes are controlled by strict change management procedures. Separation of duties for execution and approval of changes must be enforced to ensure changes cannot be made by a single individual and access control measures put in place to prevent personnel from gaining access to source code or modifying system configurations in an uncontrolled manner.
   - Vendor will apply security patches and software updates to fix vulnerabilities that put TD Auto Finance information at risk of unauthorized disclosure, misuse, alteration, destruction or other compromise. Patches must be deployed in a timely manner based on the severity of the vulnerability and the information classification of the data
   - Vendor shall ensure that all non-public personal information is sanitized from production data prior to use in development and testing systems.
   - Vendor will designate, for the duration of the Agreement, one or more individuals who ensure that information risks are being adequately addressed and technical, architectural or design decisions will not lead to violations of TD Auto Finance information security and data safeguarding requirements.

9. **Vendor Incident Management**
   - Vendor is required to investigate security incidents and provide notification to TD Auto Finance of any security incidents that could affect the confidentiality, integrity or availability of TD Auto Finance information or systems.

10. **Vendor Compliance**
    - Vendor will perform periodic internal audits to test the effectiveness of security controls and verify that it is in compliance with all regulatory, legal and contractual requirements covered by this Agreement. An Annual Statement of Compliance report will be provided to TD Auto Finance
    - TD Auto Finance reserves the right to audit the security framework of Vendor including access to the premises and data processing systems, in or on which TD Auto Finance data is used and processed in order to check the appropriateness of all technical or organizational data security measures
    - TD Auto Finance is entitled to monitor the compliance with data protection provisions and the information security measures in accordance with the requirements of this Agreement. Vendor shall provide the requested information and provide full evidence that these obligations have been met within a reasonable period
    - Vendor shall communicate the name(s) and contact data of the person(s) responsible for data protection and information security to TD Auto Finance.

Exhibit E: Compliance and Audit Requirements

1. **Compliance with Laws.** Each Party will obtain and maintain all Authorizations applicable to such Party at its own expense. Provider will comply with all Laws, including Regulatory Requirements, applicable to Provider's delivery of the Services. TDAF will comply with all Laws, including Regulatory Requirements, applicable to TDAF's receipt of Services and its performance of this Agreement. In particular, Provider will comply with applicable privacy laws.

2. **Changes in Laws.** Provider will be responsible for identifying and becoming familiar with any changes in Laws that are related to Provider's delivery or performance of the Services. TDAF will be responsible for identifying and becoming familiar with any changes in Laws that are related to TDAF's receipt and use of the Services or performance of its obligations under this Agreement.

3. **Provider Certifications.** Upon request, and at such reasonable intervals as TDAF or its auditors may specify, but not more than once in any calendar year, the Provider Contract Executive will certify to TDAF that, to the best of his or her knowledge, after reasonable inquiry: (i) its charges and reports are accurate and complete in all material respects; (ii) there are no material unbilled charges or known material unasserted claims; (iii) Provider has reported all known material breaches of security, suspected fraud or other irregularities or reportable incidents that may constitute violations of law, breaches of this Agreement or TDAF's or Provider's ethics or corporate social responsibility policies; (iv) Provider has reported to TDAF all apparent material weaknesses and deficiencies in the TDAF Controls of which Provider is aware (including, without limitation, any such controls contained in or related to the supported applications); and (v) make such other factual certifications concerning its Services and performance as TDAF or its auditors may reasonably request For purposes of these certifications, reasonable materiality standards may be specified by TDAF or its auditors

4. **Customer Certifications.** Upon request, and at such reasonable intervals as Provider or its auditors may specify, but not more than once in any calendar year, the TDAF's Contract Executive will certify to Provider that, to the best of his or her knowledge, after reasonable inquiry: (i) there are no material unbilled charges or known material unasserted claims; (ii) TDAF has reported all known material breaches of security, suspected fraud or other irregularities or reportable incidents that may constitute violations of law, breaches of this Agreement or TDAF's or Provider's ethics or corporate social responsibility policies; (iii) TDAF has reported to Provider all apparent material weaknesses and deficiencies in the TDAF Controls of which TDAF is aware (including, without limitation, any such controls contained in or related to the supported applications); and (iv) make such other factual certifications concerning its Services and performance by Provider as Provider or its auditors may reasonably request For purposes of these certifications, reasonable materiality standards may be reasonably specified by Provider or its auditors

5. **Audit.** Provider will provide TDAF, upon TDAF's request, audit support in the event TDAF, or any of its affiliates, are audited by an external authority. TDAF, its affiliates, consultants or third parties shall have the right to conduct an internal audit on Provider for all Services provided to ensure controls and process standards are maintained effectively. Nothing herein shall be deemed to grant TDAF or its auditors the right to access the Provider Services Locations or records regarding other customers of Provider. Any audits for which Provider shall provide audit support shall be conducted in a manner so as not to disrupt Provider's performance of Services and other normal operations or interfere with other customers of Provider.

6. **Control Rules.** Without limiting the generality of the foregoing and subject to this Section and the confidentiality provisions of this Agreement and TDAF's obligation to pay for same, Provider will to the extent applicable to TDAF, provide, or cause its auditor to provide, TDAF with descriptions of controls, tests of controls and audit reports to enable TDAF to fulfill its legal obligations under the Securities Act of 1933; the Securities Exchange Act of 1934; the Sarbanes Oxley Act of 2002; related rules and regulations of the Securities and Exchange Commission, including Regulation S-X; the rules, regulations and listing standards of the New York Stock Exchange; the rules, regulations and standards of the Public Company Accounting Oversight Board; and any other financial control or disclosure requirement imposed by law on public companies, as such legal requirements may be amended or modified from time to time (the "Control Rules")

(a) Provider will reasonably assist TDAF to comply with the Control Rules by: (i) placing in operation as of the Service Commencement Date and thereafter maintaining the internal controls and procedures related to the Services as agreed upon by Provider and TDAF (the "TDAF Controls"); (ii) documenting such TDAF Controls; (iii) conducting periodic internal assessments to test whether TDAF Controls are operating effectively, (iv) cooperating with TDAF and its auditor in connection with testing the effectiveness of the TDAF Controls; (vi) issuing such interim or annual certifications as TDAF may reasonably request pursuant to Section 10.3; and (vii) correcting any material weakness or significant deficiency as defined by the Control Rules or any other deficiency that would prevent TDAF from complying with the Control Rules. To the extent TDAF implements additional or alternative TDAF Controls, not less than 90 days prior to such implementation, TDAF shall notify Provider of its intent to implement such additional or alternative TDAF Controls and the Change Control Procedure described in Section 5.3 above shall be applicable to such additions or alterations.

(b) Provider will obtain a "Type II" SSAE 16 audit report including all revised reporting standards initiated by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) and the International Audit & Assessment Standards Board (IAASB); specifically SSAE 16 effective June 15, 2011, on internal controls placed in operation and tests of operating effectiveness of those controls for Provider, and any Subcontractors. Provider will provide TDAF with a copy of the Provider SSAE 16 (or revised standard) Report at no additional charge

(c) Whenever Provider obtains a SSAE 16 Audit Report, or equivalent as indicated above, they will provide TDAF with a copy of the Provider's SSAE 16 Report at no additional charge.

7. **Record Retention and Inspection.** At no additional cost to TDAF, Provider will maintain and provide reasonable access, upon TDAF's written request, to those all material data, files, records, documents and other information relating to this Agreement and the provision of the Services, and to charges and costs paid or payable by TDAF thereunder, until the latest to occur of: (i) two years from the date Provider generates a record that may be audited pursuant to this Agreement, and (ii) the expiration of such longer period as may be required under Provider's record retention policies for those records as same may be amended from time to time. At any time after expiration or termination of this Agreement, Provider may retire its retention obligation under this Section by providing a copy of such documents and records not previously delivered to TDAF in a mutually agreed format. Provider shall provide TDAF with copies of previously undelivered and requested records, documents and other information relative to the Services provided to TDAF, without additional charge to TDAF; provided, however, that if TDAF requests such data in a customized format that Provider notifies TDAF will cause Provider to incur additional expenses to Provider, TDAF shall reimburse Provider for such expenses. The records addressed in this paragraph do not include electronic data, faxes, images, paper copies, and other records or data that are the subject of the Services, and any other Confidential Information, all of which is subject to the provisions of Section 4 hereof and the applicable provisions in a particular SOW Throughout each SOW Term and for a period of 25 months after termination of such SOW, all of Provider's data, files and records referenced in the preceding paragraph may be inspected by TDAF, its duly authorized agents, representatives or employees, or by federal or state agencies having jurisdiction over TDAF or its Affiliates, at such reasonable times as TDAF may determine after giving notice to Provider and agreeing on mutually acceptable times and locations.

Exhibit F

EXHIBIT F
TD Auto Finance LLC IT General Controls

Task	Control Objective Number	Control Objective	Control Activity Number	Control Activity
SDLC	IT - PD - 100	System Development Life Cycle (SDLC) methodology has been defined and is being followed.	IT - PD - 100 - 001	IT management applies a defined system development life cycle (SDLC) methodology for the implementation of new application systems, which includes design, planning, and development, and requires user involvement in the process. The SDLC methodology also requires that new application systems be designed to include application controls to support complete, accurate, authorized, and valid transaction processing as documented in the business requirements plan.
			IT - PD - 100 - 002	A separate environment exists and is used to develop and test new application systems before migration to production.
			IT - PD - 100 - 003	New application systems are formally tested and approved (i.e. via sign-off) by IT and the business user prior to migration to production. A testing strategy is developed and followed that addresses unit, system, integration, and user-acceptance-level testing to ensure new application systems operate as intended. Testing is documented and includes, who performed the test, how the test was performed, expected results, and actual results.
			IT - PD - 100 - 004	IT Management applies a defined methodology for promoting new application systems to production.
			IT - PD - 100 - 005	Post implementation reviews are performed to verify that application controls continue to operate effectively.
Program Change	IT - PC - 100	Changes are authorized, tested and approved.	IT - PC - 100 - 006	Requests for application changes are standardized, documented, approved, and subject to formal change management procedures. Business and/or IT management formally authorize all requests for changes. Specific procedures are in place to document, authorize and approve emergency change requests.
			IT - PC - 100 - 007	Requests for operating system changes are standardized, documented, approved, and subject to formal change management procedures. Business and/or IT management formally authorize all requests for changes. Specific procedures are in place to document, authorize and approve emergency change requests.
	IT - PC - 100	Changes are authorized, tested and approved.	IT - PC - 100 - 008	Requests for database changes are standardized, documented, approved, and subject to formal change management procedures. Business and/or IT management formally authorize all requests for changes. Specific procedures are in place to document, authorize and approve emergency change requests.

Exhibit F

TD Auto Finance LLC IT General Controls

Task	Control Objective Number	Control Objective	Control Activity Number	Control Activity
Program Change			IT - PC - 100 - 009	A separate environment exists and is used to develop/test changes before migration to production.
			IT - PC - 100 - 010	Changes are formally tested and approved (i.e. via sign-off) by IT and the business prior to migration to production. Specific procedures are in place to test and approve emergency changes. A summary of testing is documented for each change including who performed the test, how was the change tested, expected test results, and actual test results.
	IT - PC - 200	Segregation of incompatible duties exist within the manage change environment	IT - PC - 200 - 011	Controls are in place to restrict migration of programs to production by authorized individuals only. IT responsibilities related to program coding and program migration from the test environment to the production environment are segregated. Segregation of these responsibilities is enforced by logical access controls, where possible, otherwise compensating controls are in place.
			IT - PC - 200 - 012	Program library software (if available), or manual procedures, log all changes migrated to production (audit trail).
Access Controls	IT - AC - 100	User access is authorized and appropriately established.	IT - AC - 100 - 013	All requests for additions or changes to access require a formal documented request and approval by an authorized approver (supported by an authorized approvers list).
			IT - AC - 100 - 014	Preventative controls are in place to ensure access to critical transactions is restricted and that segregation of duties conflicts within the application are not introduced when granting or changing access rights for all users.
			IT - AC - 100 - 015	IT performs timely actions (as defined by company policy) to ensure access rights for applications systems are removed as a result of employee termination or a change in the employee role, as informed by the business.
			IT - AC - 100 - 016	IT performs timely actions (as defined by company policy), to ensure access rights to operating systems are removed as a result of employee termination or a change in the employee role, as informed by the business, or IT management as appropriate.
			IT - AC - 100 - 017	IT performs timely actions (as defined by company policy), to ensure access rights at the database level are removed as a result of employee termination or a change in the employee role, as informed by the business, or IT management as appropriate..
			IT - AC - 100 - 018	A review of all access privileges for all users is performed on a periodic basis (as defined by company policy) for applications systems. A detailed process to perform the periodic review is documented. Any removal of access rights based upon the review are performed in a timely manner.

Exhibit F

TD Auto Finance LLC IT General Controls

Task	Control Objective Number	Control Objective	Control Activity Number	Control Activity
Access Controls	IT - AC - 100	User access is authorized and appropriately established.	IT - AC - 100 - 019	A review of all access privileges for all users is performed on a periodic basis (as defined by company policy) for operating systems. A detailed process to perform the periodic review is documented. Any removal of access rights based upon the review are performed in a timely manner.
			IT - AC - 100 - 020	A review of all access privileges for all users is performed on a periodic basis (as defined by company policy) at the database level. A detailed process to perform the periodic review is documented. Any removal of access rights based upon the review are performed in a timely manner.
			IT - AC - 100 - 021	Shared and generic IDs for applications, are limited in use, have a valid business purpose, and access is controlled.
			IT - AC - 100 - 022	Shared and generic IDs for operating systems are limited in use, have a valid business purpose, and access is controlled. The business owner ensures the process for the usage of shared and generic IDs is followed.
			IT - AC - 100 - 023	Shared and generic IDs for databases are limited in use, have a valid business purpose, and access is controlled. The business owner ensures the process for the usage of shared and generic IDs is followed.
Access Controls	IT - AC - 200	Password settings are appropriate.	IT - AC - 200 - 024	User ID and password parameters for applications systems are configured to meet or exceed company defined requirements for minimum password lengths, periodic forced password changes, account disabling after a certain number of unsuccessful login attempts, forced password change upon initial login, and password structures requiring uppercase letters, lowercase letters, and numbers.
			IT - AC - 200 - 025	User ID and password parameters for operating systems are configured to meet or exceed company defined requirements for minimum password lengths, periodic forced password changes, account disabling after a certain number of unsuccessful login attempts, forced password change upon initial login, and password structures requiring uppercase letters, lowercase letters, and numbers.
			IT - AC - 200 - 026	User ID and password parameters for databases are configured to meet or exceed company defined requirements for minimum password lengths, periodic forced password changes, account disabling after a certain number of unsuccessful login attempts, forced password change upon initial login, and password structures requiring uppercase letters, lowercase letters, and numbers.
			IT - AC - 300 - 027	System security settings for applications systems are reviewed on a periodic basis (as defined by company policy) to ensure they comply to company standards. If any deviations exist, a written explanation is completed identifying the compensating controls and is approved by Information Security.

Exhibit F

TD Auto Finance LLC IT General Controls

Task	Control Objective Number	Control Objective	Control Activity Number	Control Activity
	IT - AC - 300	General system security settings are appropnate.	IT - AC - 300 - 028	System security settings for operating systems are reviewed on a periodic basis (as defined by company policy) to ensure they comply to company standards. If any deviations exist, a written explanation is completed identifying the compensating controls and is approved by Information Security.
			IT - AC - 300 - 029	System security settings for databases are reviewed on a periodic basis (as defined by company policy) to ensure they comply to company standards. If any deviations exist, a written explanation is completed identifying the compensating controls and is approved by Information Security.
Access Controls	IT - AC - 400	Access to privileged functions is limited to appropriate individuals.	IT - AC - 400 - 030	Super users for applications are limited in number. Users with super user access privileges are appropriate based on job responsibility.
			IT - AC - 400 - 031	Super users of operating systems are limited in number. Users with super user access privileges are appropnate based on job responsibility.
			IT - AC - 400 - 032	Super users at the database level are limited in number. Users with super user access privileges are appropriate based on job responsibility.
	IT - AC - 600	Physical access to computer hardware is limited to appropriate individuals.	IT - AC - 600 - 036	Appropnate physical security and access control measures are established for the IT Data Center. Access is restricted to individuals who are authorized to gain such access. Procedures are in place to grant, change, or remove access to the IT Data Center. All actions require formal approval by an authorized approver (supported by an authorized approvers list). Documentation of the access request and approval is retained.
			IT - AC - 600 - 037	A review of all personnel with access to IT Data Center is performed on a periodic basis (as defined by company policy). A process to perform the periodic review is documented.
			IT - AC - 600 - 038	A process is in place whereby a visitor log is kept for all visitors who are granted access to the IT Data Center. Temporary visitors must be escorted if deemed appropriate.
Operations	IT - OP - 100	Job Schedules are controlled and monitored.	IT - OP - 100 - 039	Users with access to job schedules at the all operating system levels are limited in number. Users with access privileges to modify jobs are appropriate based on job responsibility.
			IT - OP - 100 - 040	Users with access to job schedules at the database level are limited in number. Users with access privileges to modify jobs are appropriate based on job responsibility.
			IT - OP - 100 - 041	Users with access to job schedules at the all application level are limited in number. Users with access privileges to modify jobs are appropriate based on job responsibility.

Exhibit F

TD Auto Finance LLC IT General Controls

Task	Control Objective Number	Control Objective	Control Activity Number	Control Activity
			IT - OP - 100 - 042	A procedure exists to monitor and control job behavior. Evidence of the review of jobs is maintained, Incidents are addressed or transferred to the correct support staff member and resolved In a timely manner.
	IT - OP - 200	Financial data is backed up and Is recoverable.	IT - OP - 200 - 043	A backup strategy has been implemented for data and programs.
			IT - OP - 200 - 048	The company's back up of financial data is stored offsite.
			IT - OP - 200 - 049	The restoration of backed up financial data is periodically tested.
Service Providers External	IT - SP - 100	Controls over third-party (external) service providers are in place.	IT - SP - 100 - 044	IT Management and Information Security obtain a copy of the third-party service provider's SSAE report for review and draws a conclusion on the adequacy of the service provider's IT general controls. If a SSAE report is not available, other appropriate evidence is obtained or other procedures are performed to assess the operating effectiveness of IT general controls at the service provider organization.
			IT - SP - 100 - 045	IT Management maintains and evaluates controls over the dataflow to and from the external service provider and performs reasonability checks on results (I.e. input/output controls).
Service Providers Internal	IT - SP - 200	Controls over internal service providers are in place.	IT - SP - 200 - 046	ITM Infrastructure Management obtains a copy of the internal service providers SOX self-assessment and reviews results.
			IT - SP - 200 - 047	ITM Infrastructure Management maintains and evaluates controls over the dataflow to and from the internal service provider and performs reasonability checks on results (I.e. Input/output controls).